



Received & Inspected

FEB 25 2010

FCC Mail Room

123 West 7th Street • Blue Earth, MN 56013
507-526-5156 • 1-877-864-5156 • Fax: 507-526-4963
www.bevcomm.net

February 19, 2010

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Suite TW-A325
Washington, DC 20544

Re: **2009 CPNI Certification and Statement of Compliance for**

Cannon Valley Cablevision, Inc. FRN 0007618929

Dear Ms. Dortch:

I enclose an original and four (4) copies of the 2009 CPNI Certification and Statement of Compliance for Cannon Valley Cablevision, Inc. As a pure reseller of interconnected VoIP service through Onvoy, Inc., this company does not have a Form 499 Filer ID number. All 499 forms for this entity are filed by Onvoy.

One copy of this filing has been mailed to Best Copy and Printing, Inc., as required by the FCC.

Very truly yours,

James L. Beattie
Assistant General Counsel

JLB: mo

Enclosures

cc: Best Copying and Printing, Inc.

No. of Copies rec'd
LFC ABOVE

0+4

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Received & Inspected

FEB 25 2010

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

1. Date filed: February 19, 2010
2. Name of company(s) covered by this certification: Cannon Valley Cablevision, Inc.
3. Form 499 Filer ID: Company does not have one as it resells the interconnected VoIP service of Onvoy, Inc., but has an FRN 0007618929
4. Name of signatory: William V. Eckles
5. Title of signatory: President and Chief Executive Officer
6. Certification:

I, William V. Eckles, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI. The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures

STATEMENT OF COMPLIANCE

The operating procedures of Rural Communications and its affiliated subsidiaries BEVCOMM, Inc., Blue Earth Valley Telephone Company, Cannon Valley Cablevision, Inc., Cannon Valley Telecom, Inc., Easton Telephone Company, Eckles Telephone Company and Minnesota Lake Telephone Company ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

Use of CPNI in Marketing

Our company has the capability to access, but does not use, CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

Our company makes limited, at the request or inquiry by a customer who has opted out, one-time use of CPNI to market our communication-related services only in compliance with FCC Rule 64.2008.

Our company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to any use of CPNI. Each customer's record contains a designation identifying whether or not we have obtained, through the processes permitted by the FCC's rules, the customer's approval to use, disclose or permit access to his or her CPNI.

Our company accesses and uses a customer's CPNI, upon the customer's inquiry about a particular communications-related service or services, to market our own (or our affiliates') communication-related services (outside a customer's current relationship) only after the customer's Opt-Out consent has been obtained in compliance with FCC Rule 64.2008, and which consent has not been revoked by the customer. Every two years our company (a) provides notice of customers' rights to restrict use and disclosure of, and access to, their CPNI, in compliance with FCC Rule 64.2008, and (b) solicits Opt Out consent for the use of the customer CPNI, in compliance with FCC Rule 64.2008, to each customer who has given Opt Out consent.

Our company prohibits access to and use of a customer's CPNI by third parties in order to market their communication-related services.

Our company has a supervisory review process regarding our compliance with the FCC's CPNI rules for any outbound marketing efforts, should we choose to use customer CPNI for such marketing efforts in the future. We require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval.

CPNI Safeguards

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company establishes passwords with customers in order to authenticate customers. Neither passwords nor the backup method for authentication rely on customers' readily available biographical information.

Our company has established password protection for customers' online accounts.

Our company includes terms specifying the confidentiality and use of CPNI in its contracts with business customers that are served by a dedicated account representative.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication, online account, or address of record.

CPNI Recordkeeping and Reporting

Our company maintains a record of our own and our affiliates' sales and marketing campaigns that use customer CPNI. We also maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. We maintain these records for at least one year.

Our company maintains records of our compliance with the FCC's CPNI Rules for use of CPNI in outbound marketing efforts, for at least one year.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.